Amendments to the Claims:

This listing of the claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method including: ~~steps of~~

providing a system including a playback device;

sending ~~a text-based message~~ to a hand-held device, via a transport technique not including the playback device, ~~using an SMS technique, the text-based message including information~~ a text-based message that includes data from which rights information is derivable by the system; ~~a system including a playback device; and~~

enforcing ~~that~~ the rights information on the system in response to ~~that~~ the text-based message

~~wherein the steps of sending include a transport technique not including the playback device~~.

2. (Currently Amended) A method as in claim 1, including steps of ensuring that only authorized content is executed or presented by the playback device or ~~the~~ a secure processor, or by both in combination or conjunction.

3. (Original) A method as in claim 1, including steps of sending content to the playback device using a communication link not used by the steps of sending a text-based message.

4. (Original) A method as in claim 1, wherein the steps of enforcing are performed at least in part by the playback device or a secure processor coupled thereto.

5. (Original) A method as in claim 1, wherein the steps of enforcing are performed by mandatory security hardware or mandatory security software.

6. (Original) A method as in claim 1, wherein the steps of enforcing include steps of decrypting at least some information derivable from the text-based message.

7. (Original) A method as in claim 1, wherein the steps of enforcing includes using a key derived from the message for decrypting a license or content.

8. (Currently Amended) A method as in claim 1, wherein the steps of enforcing includes:

putting together at least an identity of the playback device and an identity of content;

applying at least part of the message, the identity of the playback device, and the identity of the content to authenticate the execution rights for the playback device for the content ~~a key derived from the message to complete a license in which execution rights are defined~~.

9. (Original) A method as in claim 1, wherein the steps of enforcing includes applying a key derived from the message as an authentication code.

10. (Currently Amended) A method as in claim 1, wherein the message is composed on ~~the~~ an SMS.

11. (Currently Amended) A method as in claim 1, wherein at least a portion of the message is manually entered into the playback device.

12. (Currently Amended) A method as in claim 1 ~~11~~, wherein at least a portion of the message is provided to the playback device, wherein the playback device processes the portion of the message and produces a licensing message suitable to be sent by the hand-held device, and wherein the licensing message is provided to the hand-held device.

13. (Original) A method as in claim 12, wherein the licensing message is encrypted or cryptographically authenticated by the hand-held device and sent to a license server.

14. (Currently Amended) A method as in claim 1, wherein the steps of enforcing include steps of using a decryption key available to the ~~by the~~ playback device or a secure processor coupled thereto.

15. (Currently Amended) A method as in claim 1, wherein said text-based message is a first message, further comprising: ~~the steps of sending a text-based message include steps of~~

sending a ~~first~~ second message from [[a]] the hand-held device ~~using an SMS technique~~ to a license server;

sending ~~a second~~ the first message from the license server to the hand-held device, the ~~second~~ first message including human-readable characters;

~~and~~ manually entering those characters to an input element coupled to the playback device.

16. (Original) A method as in claim 1, wherein the system includes a closed content distribution system capable of delivering content to the playback device using a second transport technique not including that used by the steps of sending a text-based message.

17. (Original) A method as in claim 1, wherein the system includes a closed content distribution system capable of ensuring that only authorized content is presented by the playback device or executed by the secure processor.

18. (Original) A method as in claim 1, wherein the text-based message includes an authentication code; and the system includes a secure processor capable of authenticating content coupled to the playback device in response to that authentication code.

19. (Currently Amended) A method as in claim 1, including steps of authenticating the ~~right~~ rights information by the playback device or a secure processor coupled thereto.

20. (Currently Amended) A method as in claim ~~19~~ 1, further comprising ~~wherein the steps of authenticating include steps of~~ decrypting at least some information derivable from ~~that~~ the text-based message.

21. (Currently Amended) A method as in claim ~~19~~ 1, further comprising ~~wherein the steps of authenticating include steps of~~ using a decryption key available to the ~~by the~~ playback device or a secure processor coupled thereto to authenticate the rights information.

22. (Currently Amended) A method as in claim 1, wherein the text-based message includes characters, further comprising: ~~including steps of~~

decoding ~~those~~ characters included in the text-based message; ~~and~~

deriving rights information from at least some of those characters.

23. (Original) A method as in claim 22, wherein the steps of deriving are performed at least in part by the playback device or a secure processor coupled thereto.

24. (Original) A method as in claim 22, wherein those characters include at least some information encrypted using a key available to the playback device or a secure processor coupled thereto.

25. (Currently Amended) A method comprising: ~~including steps of~~

sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable by a system including a playback device ~~including at least one of rights-enforcing hardware, rights-enforcing software~~;

~~enforcing that rights information on the system using the rights-enforcing hardware or rights-enforcing software, in response to that text-based message.~~

putting together, at the playback device, at least an identity of the playback device and an identity of content;

applying at least part of the message, the identity of the playback device, and the identity of the content to authenticate the execution rights for the playback device for the content.

26. (Currently Amended) A method as in claim 25, wherein the playback device includes at least one of rights enforcing hardware, rights enforcing software, further including: ~~including steps of authenticating that~~

authenticating the rights information using the rights-enforcing hardware or rights-enforcing software

enforcing the rights information on the system using the rights enforcing hardware or rights enforcing software, in response to the text-based message.

27. (Original) A method including steps of

sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable by a system including a secure processor and a playback device under control of that secure processor;

authenticating that rights information at the secure processor in response to mandatory security software executed by the secure processor; and

enforcing that rights information on the system in response to that text-based message.

28. (Original) A method as in claim 27, including steps of sending content to the playback device using a communication link not used by the steps of sending a text-based message.

29. (Original) A method as in claim 27, wherein the steps of sending a text-based message include a transport technique not including the playback device.

30. (Original) A method as in claim 27, wherein the steps of sending a text-based message include steps of

sending a first message from a hand-held device using an SMS technique to a license server;

sending a second message from the license server to the hand-held device, the second message including human-readable characters; and

entering those characters to an input element coupled to the secure processor.

31. (Original) A method as in claim 27, wherein the system includes a closed content distribution system capable of delivering content to the playback device using a second transport technique not including that used by the steps of sending a text-based message, the closed content distribution system including the mandatory security software being responsive to a private key in a public-key cryptosystem.

32. (Original) A method as in claim 27, wherein the system includes a closed content distribution system capable of ensuring that only authorized content is presented by the playback device or executed by the secure processor.

33. (Original) A method as in claim 27, wherein

the text-based message includes an authentication code; and

the system includes a secure processor capable of authenticating content coupled to the playback device in response to that authentication code.

34. (Currently Amended) A method comprising: ~~including steps of~~

sending to a hand-held device using an SMS technique a signature over a token including a playback device identity and content identity; ~~a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable by a system including a playback device under control of a secure processor;~~

providing the signature to the playback device identified in the token;

enforcing, using security software at the playback device, a check against the playback device and the content identified in the token. ~~that rights information at the secure processor; and~~

~~at least one of the steps of~~

~~(A) decrypting data by the secure processor in response to a secret key and without exposing that secret key, and~~

~~(B) authenticating that rights information in response to mandatory security software executed by the secure processor.~~

35. (Currently Amended) A method comprising: ~~including steps of~~

sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable by a system including a playback device under control of a secure processor; ~~and~~

providing a signature associated with the text-based message to the secure processor;

enforcing ~~that~~ the rights information at the secure processor using the signature and an identity of the playback device.

~~wherein the steps of enforcing that rights information include one or more of the steps of~~

~~(A) the secure processor receiving a decryption key for content delivered to the playback device, the decryption key being itself encrypted using a private key available only to the secure processor,~~

~~(B) the secure processor authenticating that rights information in response to a digital signature or secure hash thereof,~~

~~(C) the secure processor receiving a shared key for rights information delivered to the secure processor, and the secure processor authenticating that rights information in response to that shared key, and~~

~~(D) the secure processor receiving a shared key for content delivered to the playback device, and the secure processor authenticating that content in response to that shared key.~~

36. (Currently Amended) A method comprising: ~~including steps of~~

~~delivering~~ providing, in a closed content distribution system, an SMS text message that includes license information ~~in a closed content distribution system~~, the closed content distribution system including a playback device and a secure processor, wherein the SMS message is sent via ~~the steps of delivering including~~ a communication link not including the playback device or secure processor~~, the communication link including a short text messaging system~~;

constructing, at the playback device, parameters of possible execution rights;

using at least part of the SMS text message as a signature to authenticate the constructed parameters of possible execution rights;

ensuring that only authorized content is executed or presented by the playback device or the secure processor, or by both in combination or conjunction~~; and~~ in accordance with the constructed and authenticated parameters of possible execution rights;

ensuring that rights information derivable from the license information is enforced by the playback device or the secure processor, or by both in combination or conjunction.

37. (Original) A method as in claim 36, including steps of authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction.

38. (Original) A method as in claim 36, including steps of determining in response to the rights information whether the user is authorized to execute or present the selected content.

39. (Original) A method as in claim 36, including steps of encoding the license information using a digital signature, secure hash, or shared secret; and

authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction, in response to the digital signature, secure hash, or shared secret.

40. (Original) A method as in claim 36, including steps of receiving content at the playback device.

41. (Original) A method as in claim 36, wherein at least a portion of the content is included on physical media transported to the playback device or secure processor.

42. (Original) A method as in claim 36, wherein at least a portion of the content is present at the playback device or secure processor before the steps of delivering license information.

43. (Original) A method as in claim 36, wherein the communication link includes a cellular telephone.

44. (Original) A method as in claim 36, wherein the content can be executed or interpreted by the playback device or the secure processor, or by both in combination or conjunction.

45. (Original) A method as in claim 36, wherein the content can be presented in a human-sensible form by the playback device or the secure processor, or by both in combination or conjunction.

46. (Original) A method as in claim 36, wherein the secure processor includes a computing device capable of enforcing mandatory execution of selected security software.

47. (Original) A method as in claim 36, wherein the secure processor includes a computing device capable of general purpose processing.

48. (Currently Amended) A method as in claim 36, wherein the steps of ~~delivering~~ providing include steps of sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable.

49. (Original) A method as in claim 36, wherein the steps of ensuring include steps of decoding the license information;

generating at least a portion of the rights information in response to the steps of decoding; and

enforcing the rights information.

50. (Currently Amended) A method as in claim 36, including steps of performing a commercial transaction concurrently with communication between ~~the~~ a license server and ~~the~~ a user.

51. (Original) A method as in claim 50, wherein the steps of performing a commercial transaction include steps of receiving information at the license server sufficient to allow that license server to effect a purchase transaction by the user.

52. (Original) A method as in claim 50, wherein the steps of performing a commercial transaction include steps of receiving proof of purchase at the license server of a license by the user.

53. (Original) A method as in claim 36, including steps of performing mandatory security software by the secure processor.

54. (Original) A method as in claim 53, wherein the steps of performing mandatory security software include one or more of:

authenticating at least one of: a specific content element, a specific playback device or secure processor, a specific user;

enforcing comparison of an identity associated with the playback device with a tamper-proof identity available to the playback device or the secure processor, or to both in combination or conjunction;

enforcing comparison of rights information with an identity of selected content available to the playback-device or the secure processor, or to both in combination or conjunction;

enforcing computation of the secret key (using its private key and server public key) and decryption of the identities; and

enforcing verification of a signature by the license server.

55. (Currently Amended) A method as in claim 36, wherein the steps of ~~delivering~~ providing include steps of delivering a code from a license server to a user; and

manually communicating the code from the user to the playback device or the secure processor.

56. (Original) A method as in claim 55, including steps of deriving license information from the code.

57. (Original) A method as in claim 55, including steps of decrypting content in response to the code.

58. (Original) A method as in claim 55, wherein the code includes a human-readable alphabetic, alphanumeric, numeric, or other character string.

59. (Original) A method as in claim 55, wherein the code includes a representation of at least a portion of a license message.

60. (Original) A method as in claim 55, wherein the steps of communicating the code include a human input device.

61. (Original) A method as in claim 55, wherein the steps of communicating the code include an input technique not part of the closed distribution system.

62. (Original) A method as in claim 55, wherein the steps of communicating the code include an SMS protocol.

63. (Original) A method as in claim 55, wherein the steps of communicating the code include a text messaging protocol.

64. (Original) A method as in claim 55, wherein the code includes a representation of a content decryption key.

65. (Original) A method as in claim 64, wherein the closed distribution system includes a public-key cryptosystem; and

the content decryption key includes a decryption key privately associated with the content, encrypted by an encryption key publicly associated with a specific playback device.

66. (Original) A method as in claim 55, wherein the code includes a representation of an identifier of one or more of: a specific content element, a specific playback device or secure processor, and a specific user.

67. (Original) A method as in claim 66, including steps of authenticating the code, the steps of authenticating including one or more of:

determining if the code is digitally signed by a license server; and

determining if the code is encrypted by a key known commonly to both the license server and the specific user.

68. (Original) A method as in claim 66, including steps of authenticating the code, the steps of authenticating including one or more of:

determining if the code is digitally signed by a license server; and

determining if the code is encrypted by a key known commonly to both the license server and the specific playback device or secure processor, or both in combination or conjunction.

69. (Currently Amended) A system comprising: ~~Apparatus including~~

a closed content distribution system including a playback device and a secure processor;

a communication link not including the playback device or secure processor;

a license server capable of being coupled to the communication link;

wherein the playback device or the secure processor, or both in combination or conjunction, includes mandatory security software that is configured to construct parameters of execution rights, and to use at least part of the text message as a signature to authenticate the constructed parameters of execution rights.

70. (Original) Apparatus as in claim 69, wherein at least a portion of the content is included on physical media transported to the playback device or secure processor.

71. (Original) Apparatus as in claim 69, wherein the communication link includes a cellular telephone.

72. (Original) Apparatus as in claim 69, wherein the mandatory security software includes instructions authenticating the license information.

73. (Original) Apparatus as in claim 69, wherein the mandatory security software includes instructions determining in response to the rights information whether the user is authorized to execute or present the selected content.

74. (Original) Apparatus as in claim 69, wherein the mandatory security software 21 includes instructions of

encoding the license information using a digital signature, secure hash, or shared secret; and

authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction, in response to the digital signature, secure hash, or shared secret.

75. (Original) Apparatus as in claim 69, wherein

the mandatory security software includes instructions ensuring that only authorized content is executed or presented by playback device or the secure processor, or both in combination or conjunction; and

rights information derivable from the license information is enforced by the playback device or the secure processor, or by both in combination or conjunction.

76. (Original) Apparatus as in claim 69, wherein the mandatory security software includes one or more of:

instructions authenticating at least one of: a specific content element, a specific playback device or secure processor, and a specific user;

instructions enforcing comparison of an identity associated with the playback device with a tamper-proof identity available to the playback device or the secure processor, or to both in combination or conjunction;

instructions enforcing comparison of rights information with an identity of selected content available to the playback device or the secure processor, or to both in combination or conjunction;

instructions enforcing computation of the secret key (using its private key and server public key) and decryption of the identities; and

instructions enforcing verification of a signature by the license server.

77. (Original) Apparatus as in claim 69, wherein the secure processor includes a computing device capable of general purpose processing.

78. (Original) Apparatus as in claim 69, including a code delivered from a license server to a user, the code being communicated from the user to the playback device or the secure processor.

79. (Original) Apparatus as in claim 78, including a content decryption key embedded in the code.

80. (Original) Apparatus as in claim 78, including a human input device coupled to the playback device or the secure processor.

81. (Original) Apparatus as in claim 78, including license information embedded in the code.

82. (Original) Apparatus as in claim 78, including an SMS protocol message.

83. (Original) Apparatus as in claim 78, including a text messaging protocol message.

84. (Original) Apparatus as in claim 78, wherein the code includes a human-readable alphabetic, alphanumeric, numeric, or other character string.

85. (Original) Apparatus as in claim 78, wherein the code includes a representation of at least a portion of a license message.

86. (Original) Apparatus as in claim 78, wherein the code includes a representation of a content decryption key.

87. (Original) Apparatus as in claim 86, wherein

the closed distribution system includes a public-key cryptosystem; and

the content decryption key includes a decryption key privately associated with the content, encrypted by an encryption key publicly associated with a specific playback device.

88. Apparatus as in claim 78, wherein the code includes a representation of an identifier of one or more of: a specific content element, a specific playback device or secure processor, and a specific user.

89. (Original) Apparatus as in claim 88, wherein the mandatory security software includes instructions authenticating the code, the instructions including one or more of:

instructions determining if the code is digitally signed by a license server; and

instructions determining if the code is encrypted by a key known commonly to both the license server and the specific user.

90. (Original) Apparatus as in claim 88, wherein the mandatory security software includes instructions authenticating the code, the instructions including one or more of:

instructions determining if the code is digitally signed by a license server; and

instructions determining if the code is encrypted by a key known commonly to both the license server and the specific playback device or secure processor, or both in combination or conjunction.